AlixPartners
when it really matters

EXHIBIT A

INFORMATION SECURITY PROGRAM OVERVIEW IT-1000-Overview Version 3.7	
Effective Date: 07-30-2014	**Owning Department:** Information Security Team

1. Purpose

AlixPartners Information Security Program has been developed to address the need for continuous security improvements and is designed to protect AlixPartners Information Assets from internal and external threats now and into the future.

2. Scope

AlixPartners has adopted the ISO 27001 framework to manage and continually evaluate its Information Security Program.

AlixPartners Information Security Program goals are to:

- Secure the firm's and client's confidential information through risk-based methodologies
- Increase the information security awareness of AlixPartners' employees
- Design and deploy technology and processes to enable security and compliance with corporate, regulatory, and client requirements
- Enable digitization of the firm and client projects while providing security commensurate with the classification of information.
- Ensure cost-effective deployment of processes and technology to protect AlixPartners' Information Assets

3. Roles, Responsibilities and Reporting Structure

The Information Security Team reports directly to the Chief Technology Officer (CTO). This ensures that the CTO is fully informed of information security risks without filtering through other groups.

Chief Information Security Officer (CISO)

The CISO is responsible for security and risk decisions related to information and technology, which is managed through the coordination, development, implementation, and maintenance of security and risk programs. This position is responsible for assessing the firm's risk tolerance, risk profile and continuous measurement of the success of the security program elements. The CISO must have a thorough understanding of the business goals and strategic objectives of the firm. Executive support is vital.

Responsibilities

- Provide the central point of contact for all information security issues and concerns
- Hire and mentor Information Security personnel to ensure skills and experience are aligned with business objectives
- Communicate complex security requirements in business terms
- Assess Information Security personnel training needs and develop roadmaps to increase security knowledge
- Allocate resources effectively to maintain the Information Security Management System (ISMS).
- Request additional resources (as needed)
- Approve the distribution of information security policies to interested parties, as needed.
- Report on the performance of the Information Security Management System (ISMS) to the Information Security Steering Committee (ISSC).
- Propose projects to the ISSC that:
  - address risks and opportunities.
  - ensure the ISMS achieves management's objectives.
  - require implementation of security controls that prevent or reduce undesired effects of doing business.
  - provide continual improvement of information security management.
- Provide updates to the ISSC of progress and/or changes to the information security objectives.
- Review and update information security objectives as appropriate based on changing business strategies or changing information security risks/opportunities.
- Use authority to delegate security functions to staff as required.
- Maintain a documented list of the current activities used to measure the effectiveness of ISMS controls and processes as outlined in the Security Metrics document.
- Evaluate the need for action to eliminate the cause of any non-conformities.

4. Security Functional Areas

There are 5 functional areas within the Information Security Team.

4.1 Security – Architecture

The Architecture team is responsible for research, design, and deployment of advanced technology solutions and security management techniques to protect the firm's assets, including intellectual property.
Key areas of focus include:

- Identity Management
- Key Management
- Threat Modelling
- End Point Security
- Cloud Security

AlixPartners
when it really matters

Responsibilities

- Research, design and implement security controls to mitigate threats and vulnerabilities to infrastructure and information
- Interface with Security Operations to ensure design solutions are practical and feasible from an operations perspective
- Provide second-level support to complex problems encountered by Security Operations

4.2 Security – Assessment

The Assessment team infrastructure is designed, implemented and operated in accordance with applicable security standards, policies, and practices. Their primary responsibilities include operational oversight of the vulnerability management program, application security, risk assessment, validation of security pen test results, problem resolution, system documentation, and system security management and support.
Key areas of focus include:

- Application Security
  - Dynamic
  - Static
- Penetration Testing
- Vulnerability Management
- Controls Assessment
- Red Team Testing
- Compliance Assessments
  - Device Hardening
- Access Controls

Responsibilities

- Conduct information security threat analysis on new and changed application development initiatives towards design, review and incident response planning.
- Review application source code for vulnerabilities.
- Identify and explain risks associated with common application vulnerabilities, demonstrate exploitation and recommend mitigation options.
- Develop and deploy monitoring program to ensure devices are compliant to build standards.
- Report findings and work with internal resources to ensure remediation occurs within defined SLAs.
- Research and assess new threats and security alerts and recommend remedial actions.
- Develop technical documentation, including standards and standard operating procedures (SOPs)
- Develop and report on key compliance and operational metrics for the vulnerability program
- Perform periodic internal assessments of implemented security controls
- Conduct annual information security risk analysis

AlixPartners
when it really matters

4.3 Security – Governance, Risk and Compliance (GRC)

The GRC team is responsible for managing the Information Security Management System (ISMS) through the implementation and maintenance of IT policies, standards, and procedures as well as the design and implementation of security controls. They are also responsible for assessing the Firm's adherence to regulations, policies, standards, controls, and procedures that support the effective, secure and compliant use of information assets. They conduct compliance assessments and independent reviews. They also perform information risk assessments, track any identified risk, report on risk items and ensure the follow-up and closure of open risks.

Key areas of focus include:

- Policy Management
- Technical Standards
- Compliance and Regulatory Management
- Control Framework Management
- Process Improvement
- Risk Assessment and Remediation
- Communications and Security Awareness Training
- Vendor Security Monitoring and Assessments
- Business Continuity Planning and Disaster Recovery (BCP/DR)
- IT System Development Lifecycle (IT SDLC)

Responsibilities

- Coordinate development and annual review of IT policies, standards, and procedures
- Measure and report on IT's and the Firm's compliance with global IT policies, standards and procedures, regulations, and controls
- Support and manage internal and external audits and assessment activities through documentation, scheduling and collecting evidence
- Perform information security risk and vendor assessments
- Manage and coordinate regular assessments of the BCP/DR and IT SDLC programs.
- Coordinate and manage Security Training and Awareness programs
- Develop information security awareness training, educational materials and conduct new hire security awareness training

4.4 Security – Network

The Security Network team enforces applicable policies and standards defined by the Information Security Steering Committee. They also provide additional support to the security monitoring personnel.

Key areas of focus include:

- Firewalls
- Intrusion Prevention
- Virtual Private Networks (VPN)
- Two-factor authentication

Responsibilities

- Perform on-going administration of perimeter and internal firewalls, intrusion detection/prevention systems, and other security monitoring tools
- Research and assess new threats and security alerts, and recommend remedial actions
- Conduct routine hardware and software audits of all supported systems to ensure compliance with established standards, policies, procedures, and requirements
- Periodic security assessment of firewall, router, switches, VPN, SSL concentrator, and other network component security configurations
- Validation of firewall configuration and rules to maintain secure connections (internal and external)

4.5 Security – Operations

The Operations team provides security monitoring, incident response, and threat analysis for the firm. This is required as they are responsible for managing the daily activities of system event logging, IDS monitoring, data leakage prevention, and incident triage, response, and analysis. They also provide support for security investigations and incident management. They continually monitor, detect, and respond to security incidents and help improve the security posture of the firm by sharing lessons learned from responding to incidents.
Key areas of focus include:

- Security Monitoring
  - Security Information Event Management (SIEM)
  - User Behavior Analysis
  - Intrusion Detection
  - Exploration-driven (hunt unknown) and Alert-driven (monitor known)
- Incident Response
  - Incident Handling
  - Triage and incident artifact analysis
- Malware Prevention
  - Network/Email/Endpoint
- Data Loss Prevention
  - Security Investigations
  - Cloud Usage Monitoring
- Threat Intelligence and Analysis
  - Produce internal intelligence
  - Consume external intelligence
- Physical Security
  - Access Control
  - CCTV/Access Monitoring

Responsibilities

- Monitor and respond to events from intrusion detection systems and system event logs
- Perform root cause analysis of security incidents and recommend corrective action
- Research, evaluate, test, and recommend new security controls and solutions

- Maintain physical security badge access control to AlixPartners environments
- Monitor physical security alerts and assist with door security
- Research and assess malware recommending remedial actions
- Respond to and investigate DLP alerts
- Report on key compliance and operational metrics for security operations
- Identify, detect and escalate incidents as defined by incident response procedures
- Report on identified incidents

5. Security Program Features

Access Controls

Logical and physical access controls exist to maintain the confidentiality, integrity, and availability of information assets. To ensure non-repudiation, users are provided unique user ID's and are granted access based on the concept of 'need to know' and 'minimum necessary' basis. All access requests must be approved by the information or system owner. The appropriate teams then provision these requests. AlixPartners periodically reviews user access and requires system and information owners to confirm that access is still required.

Automation

AlixPartners uses automation to enhance its processes and leverages automatic threat intelligence feeds, automatic updates of threat prevention signatures, and automatic detection watchlist updates to monitor for anomalous behavior. Vulnerability scans are automated and run on a scheduled basis, and multiple automated methods are in use to improve the efficiency and effectiveness of prevention, detection, and response capabilities.

Backups

AlixPartners employs various tools and services to support recovery and restoration capabilities for the client and firm information.

Baselining

AlixPartners uses baselining techniques to enhance security detection of anomalous activity and to identify the non-standard use of our systems.

Change Management

Change management is an essential part of maintaining the integrity and availability of information. AlixPartners requires employees to submit changes through its change management process. This process requires detailed change information to be captured such as Change Description, Impact, Risk, Rollback, Dependencies, etc. This allows the Change Management Board to have a thorough understanding of a change and its benefit to make an informed decision.

Containerization and Segmentation

The firewall will not allow traffic it evaluates as a threat from one zone to another, helping to keep a threat containerized.

AlixPartners
when it really matters

Data Analytics
Security analytics tools and techniques are deployed to consume large amounts of security data to monitor, alert, and create behavioral data sets to further understand anomalous or confirmed threats.

Data Loss Prevention (DLP)
Data Loss Prevention tools are in use to monitor and identify sensitive information that is at rest, in motion and in use.

Device Hardening
AlixPartners uses a baseline configuration for all systems. The baseline consists of disabling unnecessary services and setting specific options. Device hardening is defined through Active Directory GPO policies and cannot be changed at the local system level.

Electronic Information Destruction
To securely destroy electronic information, AlixPartners uses a number of mechanisms. For physical media such as paper copies and optical media, cross-cut shredders are used. These are installed in various locations within each office. For digital storage devices, such as USB and hard drives, a secure wipe process is used. All hard drives found in multi-function printers, copiers, or scanners are destroyed by an approved vendor.

Encryption
AlixPartners utilizes full disk encryption on laptops and desktop devices to ensure lost equipment does not expose firm or client information. Network communication is encrypted with secure protocols and virtual private networks are used using secure connection methods for client remote access.

Firewalls
AlixPartners deploys a network firewall at all network perimeter locations that connect to the Internet. The firewalls are all configured with a default deny policy. This policy blocks all network connectivity unless it is explicitly allowed. The firewalls are also configured to log all traffic. Some of the firewall devices provide additional security functions such as URL filtering, malware prevention, and threat prevention.

Incident Response
AlixPartners follows a defined incident response procedure for any event that impacts the information assets. This procedure contains steps to identify an incident, assign severity levels, contain the effects of the incident, take corrective actions to remediate the incident, communicate with all relevant parties, and perform a root cause analysis assessment. The root cause assessment includes actions to protect against a recurrence of the incident.

Internal Investigations
AlixPartners follows defined processes, in addition to incident response procedures, to investigate matters that may put AlixPartners employees or information assets at risk.

AlixPartners
when it really matters

Intrusion Prevention
AlixPartners deploys Intrusion Prevention at every network perimeter location that connects to the Internet. These systems are continuously monitored and tuned to ensure the maximum detection rate of malicious activity. This solution is configured to block malicious activity and log events.

ISO 27001 Certification
AlixPartners has achieved ISO 27001 certification for select data centers in the US and Europe. The scope includes management of data analytics, application development, web hosting and litigation for Engagement Technology Services.

Malware Prevention and Detection
A defense in depth approach is used to prevent, detect, and mitigate malware. The firewall has threat protection signatures to stop malware at the network layer. Sandboxing technology is used to analyze executables for malicious behavior observed. Email prevention and detection controls are in place to prevent malicious email from being delivered and to alert when a malicious email may have been delivered, or when a user clicks on a malicious link. At the endpoint layer, multiple preventive and detective controls are in place including anti-virus, application control, and endpoint detection and response tools. These tools are continually updated with updates signatures and detection methods.

Patch Management
Reports concerning network infrastructure devices, servers, and endpoints and associated Operating System or software vulnerabilities are provided to the appropriate teams on a regular basis.

Penetration Testing and Red Teaming
AlixPartners utilizes periodic penetration and Red Team testing to evaluate its security controls and incident response processes. These tests help AlixPartners continue to improve its controls and procedures to provide an effective security program.

Physical Security
Physical security is a key consideration for all AlixPartners offices. Each facility is accessible only through badge-controlled access. Each site is monitored via security cameras deployed in strategic locations at each site. This badge access is reviewed periodically to ensure only approved personnel has access to AlixPartners offices.

Privilege Management
Administrative privileges are restricted and only provided with proper justification. Users operate with standard user privileges and only escalate privileges as necessary. User and Entity Behavior Analytics tools are in place to monitor for privilege misuse.

Risk Assessments
AlixPartners' continuously identifies, reviews and mitigates risks associated with Information Assets. Periodic risk assessments are performed as appropriate. The Network Security team also participates in risk assessments when it involves an issue with a client's infrastructure.

AlixPartners
when it really matters

Mr. John Simon
Executive Vice President and General Counsel
PG&E Corporation
77 Beale Street
San Francisco, CA 94105

January 7, 2019

Re: Agreement for Financial Advisory and Consulting Services – First Addendum

Dear Mr. Simon:

This letter represents the first addendum (the "First Addendum") to the agreement between AlixPartners, LLC, a California limited liability company ("AlixPartners") and PG&E Corporation and certain of its affiliates and subsidiaries ("PG&E" or the "Company") dated December 4, 2018 (the "Engagement Letter"). Unless otherwise modified herein, the terms and conditions of the Engagement Letter remain in full force and effect. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Engagement Letter.

The Company previously provided a retainer of $750,000.00, as set forth in Schedule 1 and in accordance with Section 2 of the General Terms and Conditions of the Engagement Letter. The parties have agreed the Company shall provide an additional retainer in the amount of $1,750,000.00 for an aggregate retainer amount of $2,500,000.00.

* * *

If these terms meet with your approval, please sign and return the enclosed copy of this First Addendum.

We look forward to our continuing relationship with you.

Sincerely yours,

ALIXPARTNERS, LLP

James Mesterharm	David Hindman	John Boken
Managing Director	Managing Director	Managing Director

Acknowledged and Agreed to:

PG&E CORPORATION, and certain of its affiliates and subsidiaries

By: _____

Its: _____

Dated: _____

AlixPartners, LLP / 909 Third Avenue / New York, NY 10022 / **T** +1 212 490 2500 / **F** +1 212 490 1344 / alixpartners.com